

Appln. No. 09/629,114
Amdt./Response dated May 20, 2004
Reply to Office action dated Nov. 21, 2003

PATENT
Customer No. 22,852
Attorney Docket No. 7451.0026-00
InterTrust Ref. No.: IT-24.1 (US)

AMENDMENTS TO THE SPECIFICATION:

Please amend the specification as follows:

Please replace the paragraph beginning at page 11, line 22, with the following amended paragraph:

For example, in one embodiment system 104 may include a special-purpose protected processing environment 288, such as that provided by an integrated circuit housed in a tamper-resistant hardware package. As shown in Fig. 2, protected processing environment 288 may include non-volatile memory 289, volatile memory 290, a processor 291, a tamper-resistant barrier 293, and a communications port 294 for communicating with other components of system 104. Use of a protected processing environment is advantageous, in that it provides an area that is shielded from unauthorized observation or modification in which to run sensitive programs and to store cryptographic keys and other information. For example, transaction processing application 112, or selected portions thereof, can be loaded into RAM 290 of protected processing environment 288 and executed by CPU 291, thus protecting the operation of transaction processing application 112 from being tampered with or otherwise modified. Additional information about implementations of a protected processing environment can be found in commonly-assigned U.S. Patent No. 5,892,900, "Systems and Methods for Secure Transaction Management and Electronic Rights Protection," issued April 6, 1999 ("the '900 patent"), and commonly-assigned U.S. Provisional Application No. 60/150,126, "Secure Processing Unit Systems and Methods," by Sibert, filed August 20, 1999, each of which is hereby incorporated by reference in its entirety.

Appln. No. 09/629,114
Amdt./Response dated May 20, 2004
Reply to Office action dated Nov. 21, 2003

PATENT
Customer No. 22,852
Attorney Docket No. 7451.0026-00
InterTrust Ref. No.: IT-24.1 (US)

Please replace the paragraph beginning at page 12, line 12, with the following amended paragraph:

In another, somewhat less-secure embodiment, transaction processing application 112 makes use of software obfuscation and other software self-defensive techniques to protect itself from undetected tampering. Additional information on suitable software obfuscation and self-defensive techniques can be found in the '900 patent, and in commonly-assigned U.S. Patent Application No. 09/095,346, entitled "Obfuscation Techniques for Enhancing Software Security," filed June 9, 1998, and commonly-assigned U.S. Patent Application No. [[____]] 09/629,546, entitled "Software Self-Defense Systems and Methods," by Horning et al., filed July 31, 2000, each of which is hereby incorporated by reference in its entirety.

Please replace the paragraph beginning at page 12, line 20, with the following amended paragraph:

In addition, system 104 might advantageously include hardware and/or software for providing secure bulk storage for sensitive bookkeeping, usage, or other information. For example, a specialized hardware database can be used, and/or relatively-secure software storage protection mechanisms (or hybrid software-and-hardware mechanisms), such as those set forth in the '900 patent and in commonly-assigned U.S. Patent Application No. [[____]] 09/617,148, entitled "Trusted Storage Systems and Methods," by Maheshwari et al., filed July 17, 2000 ("the Maheshwari application"), which is hereby incorporated by reference in its entirety.

Please replace the paragraph beginning at page 24, line 3, with the following amended paragraph:

As shown in Table 1, and as described in more detail below in connection with Fig. 7, in one embodiment acknowledgment thresholds and paid thresholds are updated in response to acknowledgments received from a clearinghouse. In contrast, in a preferred embodiment controlled thresholds are updated by special control programs. For example, a controlled threshold might be attached to a prepaid budget object, and the budget provider might use a special control program to manage the budget – e.g., to add additional funds to the prepaid budget in response to a consumer's request. This mechanism thus gives the budget provider explicit control over when and how the controlled threshold, and hence the budget, is updated. Additional information on the generation and use of control programs such as the one referred to in this example can be found in commonly-assigned U.S. Patent Application No.

[[____]] 09/628,958, entitled "Systems and Methods for Controlling, Managing, Identifying, and/or Creating Objects in a Distributed Computing Environment," by Diamond, et al, filed July 31, 2000, which is hereby incorporated by reference in its entirety.